



УКРАЇНА

(19) **UA** (11) **120342** (13) **C2**
(51) МПК (2019.01)
G09C 5/00
H04L 9/00

МІНІСТЕРСТВО РОЗВИТКУ
ЕКОНОМІКИ, ТОРГІВЛІ ТА
СІЛЬСЬКОГО ГОСПОДАРСТВА
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

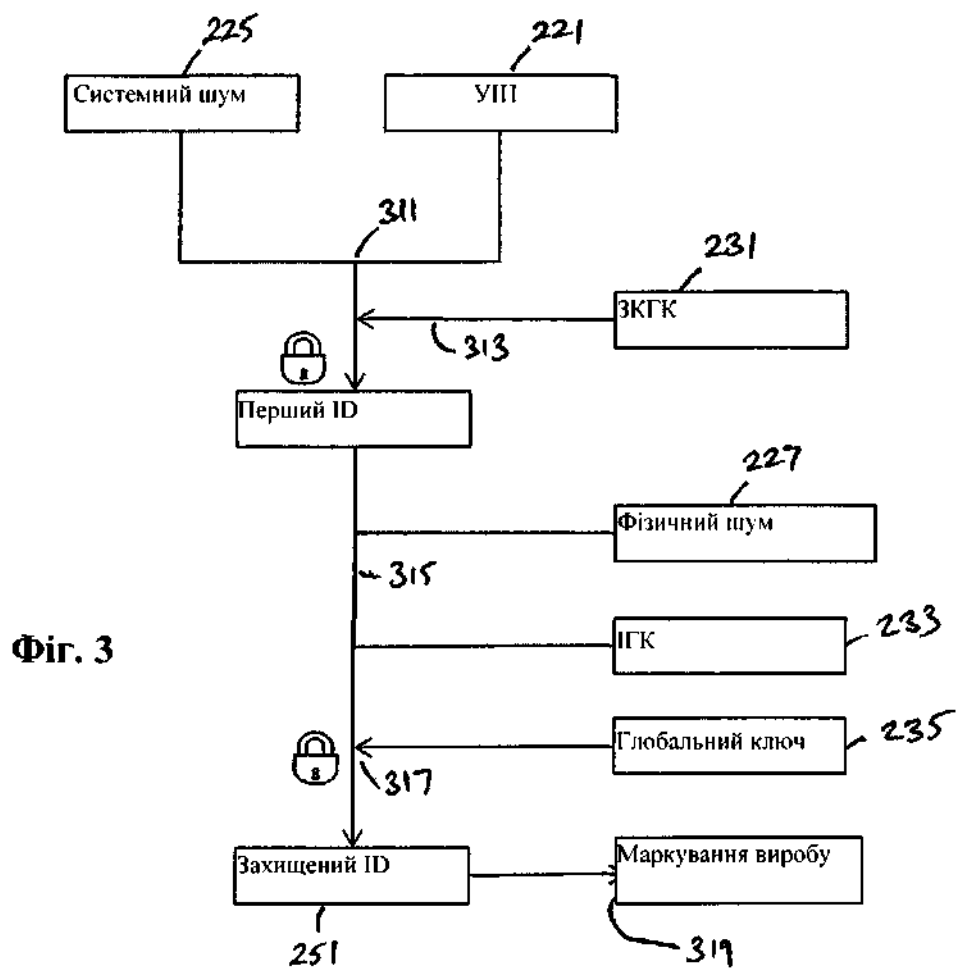
(21) Номер заявки: а 2015 05233	(72) Винахідник(и): Шане Патрік (CH), Фраде Ерван (CH)
(22) Дата подання заявки: 16.12.2013	(73) Власник(и): ІНЕКСТО СА, Avenue Edouard-Dapples 7, 1006 Lausanne, Switzerland (CH)
(24) Дата, з якої є чинними права на винахід: 25.11.2019	(74) Представник: Шляховецький Ілля Олександрович, реєстр. №190
(31) Номер попередньої заявки відповідно до Паризької конвенції: 12197525.4	(56) Перелік документів, взятих до уваги експертизою: WO 0143086 A1, 14.06.2001 WO 9724699 A1, 10.07.1997 US 6212638 B1, 03.04.2001
(32) Дата подання попередньої заявки відповідно до Паризької конвенції: 17.12.2012	
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку: EP	
(41) Публікація відомостей про заявку: 10.09.2015, Бюл.№ 17	
(46) Публікація відомостей про видачу патенту: 25.11.2019, Бюл.№ 22	
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ PCT/EP2013/076725, 16.12.2013	

(54) СПОСІБ І ПРИСТРІЙ ДЛЯ МАРКУВАННЯ ПРОМИСЛОВИХ ВИРОБІВ ЗА ДОПОМОГОЮ ФІЗИЧНОЇ ВЛАСТИВОСТІ

(57) Реферат:

Описаний спосіб маркування промислового виробу, що включає: створення унікального ідентифікатора продукту для промислового виробу; створення одного або декількох ключів шифрування; генерування таємного ключа за допомогою унікального ідентифікатора продукту та одного або декількох ключів шифрування; генерування значення системного шуму шляхом виконання хеш-функції на таємному ключі та унікальному ідентифікаторі продукту; генерування фізичного ключа з виміряної фізичної ознаки промислового виробу; генерування значення фізичного шуму шляхом виконання хеш-функції на фізичному ключі та унікальному ідентифікаторі продукту; генерування захищеного ідентифікатора, що отримано зі значення системного шуму та значення фізичного шуму або що включає їх; і розміщення відмітки на промисловому виробі, при цьому відмітка містить захищений ідентифікатор або ідентифікатор, отриманий із захищеного ідентифікатора. Також описано способи встановлення справжності виробів, маркованих згідно з описаним способом.

UA 120342 C2



Цей винахід відноситься до способів і пристрою для маркування промислових виробів. Зокрема, даний винахід відноситься до маркування упакованих товарів.

Підроблені та контрабандні товари являють собою глобальну проблему для споживачів, виробників і урядових органів. Підроблені товари, які є недозволеними виробами, як правило, більш низької якості, нелегально продають по всьому світу. Ці товари шкідливі для споживача, оскільки вони можуть бути нижчої якості, що може бути небезпечно (це особливо важливо для таких продуктів, як лікарські препарати або інші споживчі товари). Підроблені товари також шкідливі і для виробників, оскільки виробники можуть постраждати від втрати репутації, збільшення конкуренції з боку нелегальних виробників, що роблять їхні продукти, і порушення інших юридичних прав. Контрабандні товари, які виготовлено з метою уникнення податків або урядового регулювання, також є істотною проблемою для виробників і урядових органів. Ці товари нелегально перевозять, імпортують або ними нелегально торгують, що призводить до істотних втрат доходів урядових органів унаслідок неправильного збору мит або податків.

Переважно мати можливість установити справжність промислових виробів, використовуючи унікальні маркування на виробах, без потреби зберігати кожне унікальне маркування в місці, де необхідно встановити справжність виробів. Також бажано мати можливість виявляти підроблені вироби, або вироби, для яких було скопійовано унікальне маркування продукту встановленої справжності, без необхідності зберігати запис установлення справжності кожного унікального маркування.

В одній особливості винаходу передбачено спосіб маркування промислового виробу, що включає:

- створення унікального ідентифікатора продукту для промислового виробу;
- створення одного або декількох ключів шифрування;
- генерування таємного ключа за допомогою унікального ідентифікатора продукту та одного або декількох ключів шифрування;
- генерування фізичного ключа з вимірної фізичної ознаки промислового виробу;
- генерування захищеного ідентифікатора, що отримано з таємного ключа та фізичного ключа або що містить їх; і

розміщення відмітки на промисловому виробі, при цьому відмітка містить захищений ідентифікатор або ідентифікатор, отриманий із захищеного ідентифікатора.

Захищений ідентифікатор може включати унікальний ідентифікатор продукту.

Переважно, спосіб додатково включає етап генерування значення системного шуму за допомогою таємного ключа й унікального ідентифікатора продукту, при цьому захищений ідентифікатор одержують із значення системного шуму або ж він його включає. Переважно, етап генерування значення системного шуму включає виконання хеш-функції на таємному ключі та унікальному ідентифікаторі продукту.

Переважно, спосіб додатково включає генерування значення фізичного шуму за допомогою фізичного ключа й унікального ідентифікатора продукту, при цьому захищений ідентифікатор одержують зі значення системного шуму або він його включає. Переважно, етап генерування значення фізичного шуму включає виконання хеш-функції на фізичному ключі й унікальному ідентифікаторі продукту.

Відповідно до даного документа "унікальний ідентифікатор продукту" означає ідентифікатор, який унікальним чином ідентифікує промисловий виріб. Кожному промисловому виробу дають різний унікальний ідентифікатор продукту. Унікальний ідентифікатор продукту, як правило, є цифровою або буквено-цифровою послідовністю або значенням.

Відповідно до даного документа "шифрування" означає процес перетворення інформації за допомогою алгоритму, щоб зробити цю інформацію такою, яку неможливо прочитати для будь-кого, окрім тих, хто володіє особливим знанням у формі ключа. Дешифрування є зворотним процесом. "Ключ шифрування" є блоком інформації, який використовують разом з алгоритмом шифрування для шифрування або дешифрування інформації. Ключ шифрування, як правило, є цифровою або буквено-цифровою послідовністю або значенням.

Відповідно до даного документа термін "таємний ключ" використовують для опису ключа, що використовується в хеші з ключем, який генерують за допомогою унікального ідентифікатора продукту й одного або декількох додаткових ключів або блоків даних. Під час генерування таємний ключ невідомий жодній стороні, крім сторони, яка створила таємний ключ. Термін "таємний ключ" у цьому контексті не обмежено значенням закритого ключа в контексті схеми асиметричного шифрування.

Відповідно до даного документа хеш-функція представляє собою функцію, яка ставить у відповідність вхідні дані виходу фіксованого розміру (звичайно меншого, ніж вхідні дані), що називається значенням хеша. Хеш-функція, як правило, заміщає або переміщає або заміщає та

переміщає інформацію, щоб створювати значення хеша або значення шуму. Переважно, хеш-функція є криптографічною хеш-функцією. Криптографічна хеш-функція робить відбиток або контрольну суму вхідних даних. Два блоки даних можуть вважатися ідентичними, якщо при використанні однієї й тієї ж криптографічної хеш-функції вони дають однакове значення хеша.

5 Переважно, хеш-функція є однобічною хеш-функцією, що означає, що чисельно неможливо одержати вхідні дані зі значення хеша. Ці ознаки можуть використовуватись у процесі встановлення справжності відповідно до опису. Хеш-функцію може бути забезпечено ключем шляхом комбінації таємного ключа та вхідного повідомлення, щоб створювати значення хеша з ключем або шум.

10 Відповідно до даного документа термін "значення шуму" означає значення хеша або значення хеша з ключем або значення чи послідовність символів, отримані безпосередньо зі значення хеша та таємного ключа.

15 Виміряна фізична ознака промислового виробу може представляти собою будь-яку вимірну фізичну ознаку та може бути заснована на масі, розмірі, формі, текстурі або візерунку поверхні, кольорі, хімічному складі або відповіді на вхідний сигнал, такий як відповідь на електричний, магнітний або оптичний сигнал. Вимірну фізичну ознаку переважно вибирають і вимірюють до деякого розділення так, що вона, імовірно, буде унікальною для кожного виготовленого виробу або, щонайменше, більш імовірно, буде відрізнитись для будь-яких двох промислових виробів. Виміряна фізична ознака переважно передбачає фізичну сигнатуру для промислового виробу. У переважному варіанті здійснення виміряна фізична ознака представляє собою зображення частини пакунку промислового виробу.

20 Захищений ідентифікатор може представляти собою будь-який тип ідентифікатора, але переважно є цифровою або буквено-цифровою послідовністю або значенням. Відмітка також може представляти собою послідовність символів або чисел або може представляти собою графічне подання, таке як одно- або двовимірний штрих-код.

25 В одному варіанті здійснення етап генерування захищеного ідентифікатора включає генерування першого ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням системного шуму та генерування захищеного ідентифікатора шляхом шифрування першого ідентифікатора разом зі значенням фізичного шуму.

30 У цьому варіанті здійснення спосіб може додатково включати встановлення справжності виготовленого виробу в перевірочному центрі, при цьому етап встановлення справжності включає: ідентифікацію відмітки на виробі; дешифрування відмітки для одержання першого ідентифікатора та значення фізичного шуму; дешифрування першого ідентифікатора для одержання унікального ідентифікатора продукту та значення системного шуму; генерування нового фізичного ключа з вимірної фізичної ознаки виготовленого виробу; генерування нової копії значення фізичного шуму шляхом виконання хеш-функції на новому фізичному ключі та отриманому унікальному ідентифікаторі продукту; порівняння нової копії значення фізичного шуму з отриманим значенням фізичного шуму; і надання вказівки, чи ідентичне або чи корелює отримане значення фізичного шуму новій копії значення фізичного шуму.

40 Етап порівняння може включати одержання ступеня кореляції, а етап надання вказівки включає надання вказівки, чи перевищує ступінь кореляції граничне значення.

45 У цьому варіанті здійснення етап встановлення справжності може додатково включати: генерування нової копії таємного ключа з унікального ідентифікатора продукту та одного або декількох ключів шифрування; генерування нової копії значення системного шуму шляхом виконання хеш-функції на новій копії таємного ключа та унікальному ідентифікаторі продукту; порівняння нової копії значення системного шуму з отриманим значенням системного шуму; і надання вказівки, чи є ідентичними нова копія значення системного шуму та отримане значення системного шуму.

50 В іншому варіанті здійснення етап генерування захищеного ідентифікатора включає генерування першого захищеного ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням системного шуму; генерування другого захищеного ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням фізичного шуму; і розміщення відмітки на виготовленому виробі, відмітка містить перший і другий захищені ідентифікатори або ідентифікатор чи ідентифікатори, отримані з першого та другого захищених ідентифікаторів.

55 У цьому варіанті здійснення спосіб може додатково включати встановлення справжності виготовленого виробу в перевірочному центрі, при цьому етап установа справжності включає: ідентифікацію відмітки на виробі; дешифрування відмітки для одержання унікального ідентифікатора продукту, значення системного шуму та значення фізичного шуму; генерування нової копії таємного ключа з унікального ідентифікатора продукту та одного або декількох

ключів шифрування; генерування нової копії значення системного шуму шляхом виконання хеш-функції на новій копії таємного ключа та унікальному ідентифікаторі продукту; порівняння нової копії значення системного шуму з отриманим значенням системного шуму; генерування нового фізичного ключа з вимірної фізичної ознаки промислового виробу; генерування нової копії значення фізичного шуму шляхом виконання хеш-функції на новому фізичному ключі та отриманому унікальному ідентифікаторі продукту; порівняння нової копії значення фізичного шуму з отриманим значенням фізичного шуму; і наданням вказівки, чи ідентична нова копія значення системного шуму отриманому значенню системного шуму та чи ідентична або чи корелює нова копія значення фізичного шуму отриманому значенню фізичного шуму.

У кожному з цих варіантів здійснення етап генерування першого захищеного ідентифікатора може включати шифрування унікального ідентифікатора продукту та значення системного шуму за допомогою ключа генератора коду, при цьому етап генерування другого захищеного ідентифікатора включає поєднання першого захищеного ідентифікатора та значення фізичного шуму разом з ID генератора коду, і при цьому ключ генератора коду може бути отриманий або добутий з довідкової таблиці в перевірочному центрі за допомогою ID генератора коду.

У кожному з цих варіантів здійснення спосіб може додатково включати етап збереження одного або декількох ключів шифрування в перевірочному центрі. Один або кілька ключів шифрування можуть містити статичний ключ і динамічний ключ, і при цьому новий динамічний ключ створюють для кожної партії промислових виробів, тоді як той самий статичний ключ використовують для декількох партій промислових виробів.

Унікальний ідентифікатор продукту може включати інформацію, що ідентифікує партію виробів, до якої належить виріб.

Винахід передбачає здатність встановлювати справжність як на основі інформації від виробника, тобто різних ключів шифрування, так і на основі фізичної ознаки виробу. Це передбачає два рівні встановлення справжності та забезпечує виявлення клонування ідентифікаторів на даних výroбах, але не вимагає масштабного сховища кодів встановлення справжності.

В іншій особливості винаходу передбачено пристрій для маркування промислового виробу, що містить:

генератор ключа, виконаний з можливістю генерувати ключі шифрування;
генератор коду, виконаний з можливістю генерувати унікальний ідентифікатор продукту для кожного промислового виробу;

генератор фізичного ключа, виконаний з можливістю генерувати фізичні ключі з вимірної фізичної ознаки кожного промислового виробу;

засіб обробки, виконаний з можливістю:
генерувати таємний ключ для кожного промислового виробу за допомогою унікального ідентифікатора продукту й одного або декількох ключів шифрування;

генерувати захищений ідентифікатор, що отримано з таємного ключа та фізичного ключа або що містить їх; і

маркер для маркування кожного промислового виробу захищеним ідентифікатором або ідентифікатором, отриманим із захищеного ідентифікатора.

Переважно, процесор виконано з можливістю генерувати значення системного шуму для кожного промислового виробу за допомогою таємного ключа та унікального ідентифікатора продукту, при цьому захищений ідентифікатор одержують із значення системного шуму або він його включає. Переважно, процесор виконано з можливістю генерувати значення системного шуму для кожного промислового виробу шляхом виконання хеш-функції на таємному ключі та унікальному ідентифікаторі продукту.

Переважно, процесор виконано з можливістю генерувати значення фізичного шуму для кожного промислового виробу за допомогою фізичного ключа й унікального ідентифікатора продукту, при цьому захищений ідентифікатор одержують з фізичного шуму або ж він включає значення фізичного шуму. Переважно, процесор виконано з можливістю генерувати значення фізичного шуму для кожного промислового виробу шляхом виконання хеш-функції на фізичному ключі й унікальному ідентифікаторі продукту.

В одному варіанті здійснення засіб обробки виконано з можливостями: генерувати перший ідентифікатор для кожного промислового виробу шляхом шифрування унікального ідентифікатора продукту разом з таємним ключем або значенням системного шуму; і генерувати захищений ідентифікатор для кожного виготовленого виробу шляхом шифрування першого ідентифікатора разом зі значенням фізичного шуму.

В іншому варіанті здійснення засіб обробки виконано з можливостями: генерувати перший захищений ідентифікатор для кожного промислового виробу шляхом шифрування унікального

ідентифікатора продукту разом з таємним ключем або значенням системного шуму та генерувати другий захищений ідентифікатор для кожного промислового виробу шляхом шифрування унікального ідентифікатора продукту разом з фізичним ключем або значенням фізичного шуму; і маркер виконано з можливістю маркувати кожний виготовлений виріб першим захищеним ідентифікатором і другим захищеним ідентифікатором або ідентифікатором чи ідентифікаторами, отриманими з першого та другого захищених ідентифікаторів.

Промисловий виріб може бути тарою, що містить тютюновий продукт. Прикладами тютюнових продуктів є сигарети, аркушевий тютюн, сигари та картриджі або заправлення для курильних систем, що електрично нагріваються, або інших систем електронних сигарет.

Винахід дозволяє встановлювати справжність промислових виробів без вимоги сховища великих обсягів інформації. Це важливо для будь-якої практичної системи, що підходить для встановлення справжності виробів, виготовлених у великих обсягах. Крім того, використання фізичного ключа в комбінації з унікальним ідентифікатором продукту (УІП) підвищує захищеність і робить виробництво підроблених і контрабандних товарів більш складним. Додавання фізичного ключа передбачає систему, яка може виявляти клонування і є складною для копіювання. Навіть якщо фальсифікатор знає про конкретний інструмент, що використовується для генерування фізичного ключа, комбінація фізичного ключа з УІП для виробництва ідентифікатора робить клонування майже неможливим. Винахід також дозволяє проводити встановлення справжності в режимі онлайн, тобто підключається до перевірного центру по мережі зв'язку на основі значення системного шуму, а також дозволяє проводити встановлення справжності в автономному режимі на основі значення фізичного шуму. Маркування, що має бути на кожному виробі, представляє собою просто один або кілька кодів і таким чином у незначній мірі збільшує витрати на кожний виріб у порівнянні з деякими іншими рішеннями, у основі яких лежать дорогі етикетки, які технічно складно відтворити.

Далі винахід буде описано винятково на прикладах з посиланнями на супровідні графічні матеріали, у яких:

фіг. 1 — схематичний вид системи маркування відповідно до одного варіанта здійснення винаходу;

фіг. 2 представляє, як одержують значення системного шуму та значення фізичного шуму;

фіг. 3 — блок-схема, що представляє спосіб маркування одного варіанта здійснення винаходу, який може бути реалізовано в системі, представлений на фіг. 1;

фіг. 4 — блок-схема, що представляє спосіб встановлення справжності для варіанта здійснення винаходу, представленого на фіг. 3, який може бути реалізовано в системі, представлений на фіг. 1;

фіг. 5 — блок-схема, що представляє спосіб маркування згідно з іншим варіантом здійснення винаходу, який може бути реалізовано в системі, представлений на фіг. 1; і

фіг. 6 — блок-схема, що представляє спосіб встановлення справжності для варіанта здійснення винаходу, представленого на фіг. 5, який може бути реалізовано в системі, представлений на фіг. 1.

Унікальні маркування на промислових виробках можуть використовуватись для відстеження виробів. Наприклад, замовлення споживача може бути пов'язано з ідентифікуючою етикеткою або етикетками конкретного транспортного ящика або ящиків, що містять замовлені товари. "Товари" в цьому контексті означають промислові вироби або інші вироби, призначені для розподілу або продажу споживачам. Це дозволяє споживачеві, виробнику та будь-яким посередникам постійно відслідковувати місце розташування необхідних товарів. Це може досягатись за допомогою сканерів для сканування ідентифікаторів і здійснення зв'язку з перевірочним центром. Альтернативно ідентифікатори можуть зчитуватись людиною, яка може потім вручну здійснювати зв'язок із перевірочним центром. Ідентифікатори також можуть використовуватись споживачами, національними органами й іншими сторонами для перевірки того, що конкретний виріб містить справжні продукти. Наприклад, одна сторона може використовувати сканер для зчитування ідентифікатора на транспортному ящику (або ідентифікатор може бути зчитаний людиною, як зазначено вище). Деталі ідентифікатора можуть відправлятися у перевірочний центр. Перевірочний центр потім може переглядати або іншим способом обробляти деталі ідентифікатора, визначати деталі виробництва транспортного ящика та відправляти ці деталі на сканер, у такий спосіб дозволяючи стороні підтверджувати, що транспортний ящик і продукти в ньому є справжніми. Якщо центральна база даних не розпізнає ідентифікатор, сторона може вважати, що розглянуті вироби є підробленими. Ідентифікатори також можуть використовуватись для відстеження виробів. Наприклад, якщо виробнику потрібно відкликати продукти з обраної кількості транспортних ящиків, ці транспортні ящики можна відстежити за допомогою їх ідентифікаторів.

На фіг. 1 представлено схематичний вид системи маркування відповідно до одного варіанта здійснення винаходу. У цьому варіанті здійснення система 101 містить один або кілька виробничих центрів 103, 105, 107 для виробництва промислових виробів 109. Кожний виробничий центр може містити виробничу лінію або устаткування, яке може бути лінію виготовлення та упакування сигарет. Переважно, виробництво здійснюють партіями, кожна партія призначена для виробництва певної кількості окремих промислових виробів. За наявності двох або більшої кількості виробничих центрів вони можуть бути фізично розташовані на одному або різних промислових майданчиках. У цьому переважному варіанті здійснення система містить виробничі центри 103, 105, 107, але винахід може насправді бути здійснено в пункті імпорту, пункті розподілу, у покупця, оптового торговця або будь-якому іншому пункті в ланцюзі поставки.

Кожний виробничий центр містить генератор 111 коду для генерації кодів для промислових виробів 109. Переважно, генератор 111 коду представляє собою повністю автономний комп'ютер або мікроконтролер, призначений для конкретного виробничого центру. Кожний виробничий центр також містить генератор 112 фізичного ключа, який вимірює або шифрує фізичну ознаку кожного промислового виробу та перетворює його у фізичний ключ 207. Генератор 111 коду використовує фізичні ключі для генерування кодів для маркування на виробах.

У цьому варіанті здійснення генератор фізичного ключа має тип, описаний в WO2007/071788. Частина пакунку кожного виробу освітлюють, і цифровий датчик зображення захоплює зображення освітленої частини. Частина пакунку вибирають за її стабільну в часі, безладну мікроструктуру. Матеріали, такі як папір і картон, мають безладну мікроструктуру, яка може використовуватись як "відбиток" виробу. Зображення мікроструктури частини виробу перетворюють у фізичний ключ або сигнатуру, як описано в WO2007/071788, у формі буквено-цифрового значення або матриці. Генератор фізичного ключа цього типу доступний в Signoptic Technologies, Savoie Technolac, 5 allée Lac d'Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, France (Франція). Проте використовуватись може будь-який тип генератора фізичного ключа, і його може бути засновано на інших фізичних ознаках виробу, таких як маса або форма, або може навіть бути засновано на хімічних або біологічних ознаках виробу.

У цьому варіанті здійснення кожний виробничий центр також містить маркер 113 для маркування згенерованих кодів на промислові вироби 109. Маркер 113 може містити будь-який підходящий маркувальний засіб, наприклад, але без обмеження, безперервний струминний принтер, краплинно-імпульсний струминний принтер, голографічний принтер, лазерний принтер або будь-який інший принтер або маркер, який дозволяє друкувати або маркувати згенеровані коди на окремих промислових виробах. Друкування або маркування згенерованих кодів може здійснюватись на кожному виробі, на зовнішньому пакунку, на етикетках або будь-яким іншим зручним способом. В одному варіанті здійснення згенеровані коди друкують на клейких мітках або етикетках, які повинні бути накладені на промислові вироби, переважно без можливості знімання. В одному варіанті здійснення згенеровані коди друкують лазерним променем на шарі чутливого до лазера матеріалу, нанесеного на виробничий виріб на пакунку виробу. Цей спосіб дозволяє друкувати код через прозорий обгортковий шар.

Система 101 додатково містить перевірочний центр 114, який містить генератор 115 ключа для генерації ключів 209, 211 для використання в маркуванні та встановленні справжності промислових виробів, і центральний сервер 117. У цьому варіанті здійснення генератор 111 коду може здійснювати зв'язок із перевірочним центром 114 через захищене інтернет-з'єднання 119 і сервер 121, локальний для виробничого центру, або за допомогою інших способів передачі даних. Альтернативно, генератор 111 коду може здійснювати зв'язок із перевірочним центром через виробничий портал, призначений для одного або декількох виробничих центрів.

Генератор 115 ключа генерує криптографічний ключ, який у даному документі називається статичним ключем. Генератор 115 ключа генерує незашифровану версію статичного ключа та зашифровану версію статичного ключа. Незашифрована версія статичного ключа, яка в даному документі називається активним статичним ключем 209, представлена на фіг. 1 суцільною границею. Зашифрована версія статичного ключа, яка в даному документі називається пасивним статичним ключем 211, представлена на фіг. 1 пунктирною границею. Активний статичний ключ 209, тобто незашифровану версію статичного ключа, генерують у генераторі 115 ключа, і тому він доступний центральному серверу 117. Генератор 115 ключа відправляє пасивний статичний ключ 211 генератору 111 коду у виробничому центрі 103, 105, 107.

Пасивний статичний ключ 211 може бути відправлено з генератора 115 ключа генератору 111 коду на постійному запам'ятовувальному пристрої, наприклад CD-диску, DVD-диску або знімному жорсткому диску. Запам'ятовувальний пристрій фізично переносять на генератор 111

коду у виробничому центрі 103, 105, 107. Альтернативно, пасивний статичний ключ 211 може бути відправлено з генератора 115 ключа генератору 111 коду через захищене інтернет-з'єднання, наприклад таке, у якому використовується шифрування. Це може бути за запитом від генератора 111 коду. Це гарантує справжність, конфіденційність і цілісність статичного ключа.

5 Генератор 115 ключа також генерує код 213 активації, який містить ключ або код для дешифрування пасивного статичного ключа 211 для формування активного статичного ключа 209. Цей код 213 активації також доступний центральному серверу 117. Переважно, активний статичний ключ 209 і код 213 активації зберігають разом з ідентифікацією виробничого центру 103, 105, 107, якому їх виділяють.

10 В одному варіанті здійснення статичний ключ містить ряд частин. Основна частина може представляти собою кілька таємних кодів, наприклад складний вираз. Складний вираз може бути, наприклад, довгим рядком випадкових або псевдовипадкових цифр або символів. Ряд частин може додатково включати унікальний ідентифікатор для статичного ключа, упорядкований код, що визначає, як статичний ключ необхідно сполучати з динамічним ключем (обговорюється нижче), цифровий криптографічний сертифікат, пов'язаний з унікальним ідентифікатором статичного ключа, і правила або ліцензію статичного ключа, які містять цифровий криптографічний сертифікат, згенерований вище.

Переважно, пасивний статичний ключ, тобто зашифровану версію статичного ключа, і особливо кілька таємних кодів, шифрують за допомогою стійкого шифру. Прикладом підходящого шифру є блоковий шифр із потрійним DES (Стандарт шифрування даних) або блоковий шифр із потрійним DES/Пендал. Обидва застосовують алгоритм шифрування Стандарту шифрування даних три рази до кожного блоку даних, і потрійний DES/Пендал є варіантом потрійного DES із незначними змінами, який був розроблений IBM. У цьому випадку ключ потрійного DES або потрійного DES/Пендал містить код 213 активації. Таким чином, у переважному варіанті здійснення активний статичний ключ 209 незашифрований, пасивний ключ 211 зашифрований за допомогою ключа потрійного DES або потрійного DES/Пендал, і код 213 активації містить цей ключ потрійного DES або потрійного DES/Пендал.

На наступному етапі 203 реєструють пасивний статичний ключ 211, отриманий генератором 111 коду. Це здійснюється генератором 111 коду, що відправляє у перевірочний центр 114 інформацію 215 про отриманий статичний ключ і будь-яку зв'язану машинну інформацію (не показана). Її переважно відправляють через захищене інтернет-з'єднання 119, як презентовано на фіг. 1, але можуть відправляти іншим підходящим способом. Перевірочний центр 114 відправляє назад генератору 111 коду код 213 активації. Код 213 активації дозволяє активувати пасивний статичний ключ 211, і це схематично представлено на 217. Код 213 активації переважно також відправляють по захищеному інтернет-з'єднанню 119, як показано на фіг. 1. Процедура реєстрації переважно організована так, що активний статичний ключ 209 ніколи не передають по Інтернету.

Процедура реєстрації може мати форму звичайного механізму обміну пари відкритий/закритий ключ. Вона може використовувати асиметричну пару ключів, пов'язану з цифровим криптографічним сертифікатом, що утворює частину статичного ключа, як обговорювалося вище. У цьому випадку відкритий ключ асиметричної пари ключів може мати форму ключа, виданого третьою стороною, наприклад урядовим органом. Інформація 215 про отриманий статичний ключ, яка відправляється з генератора 111 коду в перевірочний центр 114, може містити унікальний ідентифікатор для статичного ключа, який утворює частину статичного ключа, як обговорювалося вище. Відповідна машинна інформація (не показана), яку також відправляють із генератора 111 коду в перевірочний центр 114, може містити унікальний ідентифікатор або сертифікат для генератора 111 коду або виробничого центру. Цей унікальний ідентифікатор може включати інформацію про місце розташування та ідентичність генератора коду або виробничого центру, який попередньо одержав дозвіл на виробництво. Переважно, унікальний ідентифікатор статичного ключа та ідентифікатор генератора коду або виробничого центру шифрують за допомогою відкритого ключа асиметричної пари ключів, пов'язаної із сертифікатом статичного ключа.

Коли перевірочний центр 114 одержує зашифрований унікальний ідентифікатор статичного ключа та ідентифікатор генератора коду або виробничого центру, перевірочний центр 114 може їх дешифрувати за допомогою закритого ключа асиметричної пари ключів, пов'язаної із сертифікатом статичного ключа. Перевірочний центр потім може перевіряти, що унікальний ідентифікатор статичного ключа та ідентифікатор генератора коду або виробничого центру є дійсними. Потім перевірочний центр 114 відправляє назад на генератор 111 коду код 213 активації. Як уже згадано, переважно, код 213 активації має форму шифру з потрійним DES або з потрійним DES/Пендал. Перевірочний центр шифрує код активації (наприклад, шифр з

потрійним DES або з потрійним DES/Пендал) з відкритим ключем асиметричної пари ключів, пов'язаної з сертифікатом статичного ключа. Це дозволяє генератору коду дешифрувати код активації (наприклад, шифр з потрійним DES або з потрійним DES/Пендал) за допомогою закритого ключа асиметричної пари ключів, пов'язаної із сертифікатом статичного ключа. Потім пасивний статичний ключ 211 може бути активовано за допомогою дешифрованого коду 213 активації, щоб сформувати активний статичний ключ 209.

Коли пасивний статичний ключ 211 у генераторі 111 коду було активовано, виробничий центр може виготовляти вироби та робити коди для промислових виробів у генераторі 111 коду.

Генератор 111 коду генерує новий ключ, який у даному документі називається динамічним ключем 219, для кожної партії промислових виробів. Динамічний ключ 219 переважно представляє собою випадковий таємний код, такий як випадкове число. Генератор коду використовує динамічний ключ 219 для партії, разом з активним статичним ключем 209, щоб генерувати таємний ключ 223. Таємний ключ 223 представляє собою n, використовуване в комбінації з фізичними ключами та унікальним ідентифікатором продукту (УІП) для кожного виробу, щоб генерувати коди 221 (наприклад, буквено-цифрові коди), які повинні бути марковані на промислових виробах у цій партії. У цьому варіанті здійснення УІП для кожного виробу містить деталі виробництва, що ідентифікують час виробництва разом зі значенням підсумовуючого лічильника, щоб розрізнити вироби, зроблені в один період часу одним виробничим центром.

Генератор коду використовує криптографічну хеш-функцію на комбінації УІП з таємним ключем і комбінації УІП з фізичним ключем. Це створює цифрові відбитки, які називаються в даному документі "значеннями шуму", для виробу, і ці значення шуму використовують для генерування кодів 221, які маркують на виробах маркером 113. На додаток до звичайно використовуваних криптографічних хеш-функцій, для генерування значень хеша або значень шуму доступно безліч способів, включаючи, але без обмеження: перетворення, заміщення, табличне заміщення та індексування.

Фіг. 2 представляє спосіб генерування значень шуму, реалізований генератором 111 коду. Для генерування значення 225 системного шуму спочатку одержують таємний ключ з активного статичного ключа 209, динамічного ключа 219 та УІП 221. Динамічний ключ 219 і активний статичний ключ 209 відомі тільки перевірконому центру 114 і генератору 111 коду. На етапі 301 динамічний ключ і УІП використовують для добування таємного ключа зі складного виразу, що міститься в статичному ключі, згідно з упорядкованим кодом у статичному ключі. Таємний ключ 223 і УІП 221 потім хешують на етапі 303, щоб робити системний шум для виробу. Для генерування значення 227 фізичного шуму фізичний ключ 207 хешують з УІП 221 на етапі 305. Хеш-функція, яку використовують для генерування значення системного шуму, може бути тією ж хеш-функцією, яку використовують для генерування значення фізичного шуму, або відрізнитись від неї.

Фіг. 3 представляє спосіб використання значення системного шуму та значення фізичного шуму для генерування захищеного ідентифікатора для кожного виробу згідно з першим варіантом здійснення винаходу. На етапі 311 значення 225 системного шуму та УІП 221 з'єднують. На етапі 313 з'єднані значення системного шуму та УІП шифрують заплутуваним ключем 231 генератора коду (ЗКГК) для виробництва першого ідентифікатора 241. ЗКГК є конкретним для генератора коду та попередньо завантажується в генератор коду. Перший ідентифікатор 241 потім з'єднують зі значенням 227 фізичного шуму та ідентифікатором 233 генератора коду. Ідентифікатор генератора коду (ІГК) 233 дозволить одержати ЗКГК під час встановлення справжності. Комбінація першого ідентифікатора, значення фізичного шуму та ІГК потім шифрують за допомогою глобального ключа 235 на етапі 317 для виробництва захищеного ідентифікатора 251. Глобальний ключ 235 є загальним для всіх виробничих центрів і може бути частиною симетричної або асиметричної пари ключів, відомої перевірконому центру. Захищений ідентифікатор 251 потім маркують на виробі на етапі 319 маркером 113.

Генератор 111 коду або виробничий центр 103, 105, 107 веде підрахунок кодів, які маркують на промислових виробах. Крім того, генератор 111 коду відправляє динамічний ключ 219 для кожної партії, разом з інформацією про партію (не показана), у перевірочний центр 114. Це може виконуватись через захищене інтернет-з'єднання 119. Інформація про партію може включати різні блоки інформації, наприклад, але без обмеження, бренд, ринок або пункт призначення. Динамічні ключі 219 непотрібно відправляти в перевірочний центр 114 у реальному часі, і вони можуть передаватися в перевірочний центр у будь-який підходящий час, наприклад щомісяця. Динамічні ключі 219, відправлені в перевірочний центр 114, зберігають у базі даних (наприклад, на центральному сервері 117) у перевірочному центрі 114 або

доступними з нього. Динамічний ключ 219 для кожної партії переважно зберігають разом з інформацією про партію, відправлену в перевірочний центр 114 у той самий час.

5 Переважно, активний статичний ключ 209 видаляють, коли генератор 111 коду в конкретному виробничому центрі 103, 105, 107 виводять із роботи. Це запобігає одержанню доступу до активного статичного ключа 209 з боку злоумисника без належної реєстрації. Може бути передбачено додаткові засоби для відключення генератора 111 коду та запобігання неавторизованому використанню генератора 111 коду та виробничого центру.

10 Фіг. 4 представляє етапи, які виконуються перевірочним центром 114 і користувачем 601, коли користувач 601 бажає встановити справжність окремого промислового виробу, маркованого згідно з процесом, представленим на фіг. 3. Користувач 601 зчитує код 221 на виробі та відправляє його в перевірочний центр 114. Це показано на фіг. 1. Користувач 601 може відправити код у перевірочний центр 114 будь-яким підходящим способом, таким як захищене або незахищене інтернет-з'єднання.

15 Перевірочний центр одержує захищений ідентифікатор на етапі 321. Захищений ідентифікатор дешифрують за допомогою глобального ключа 235 (або відповідного ключа в парі ключів, якщо використовують асиметричні ключі) на етапі 323, щоб виявити значення 227 фізичного шуму та перший ідентифікатор 241. Також виявляють ІГК. За допомогою довідкової таблиці потім одержують ЗКГК 231 з ІГК. Перший ID потім дешифрують на етапі 325 за допомогою ЗКГК 231, щоб виявити системний шум 225 і УІП 221. З цією інформацією, разом з активним статичним ключем 209, динамічним ключем 219 і новим фізичним ключем, може бути відновлено як значення фізичного шуму, так і значення системного шуму для встановлення справжності виробу.

25 Для відтворення значення фізичного шуму новий фізичний ключ повинен бути отриманий користувачем 601 на етапі 327 шляхом запису зображення частини виробу в такий же спосіб і в тих же умовах, які використані для генерування оригінального фізичного ключа 207. УІП і новий фізичний ключ потім хешують для генерування нового значення фізичного шуму на етапі 329. На етапі 331 новий фізичний шум порівнюють із витягнутим значенням фізичного шуму, виявленим на етапі 323. Якщо нове значення фізичного шуму значною мірою подібно витягнутому значенню фізичного шуму, то одна частина процесу встановлення справжності завершена. Якщо нове значення фізичного шуму незначною мірою подібно витягнутому значенню фізичного шуму, то виріб визначають як несправжній на етапі 339.

30 Щоб вважати виріб справжнім, може бути необхідно, щоб нове значення фізичного шуму було ідентичним витягнутому значенню фізичного шуму. Проте, щоб вважати виріб справжнім, можна допустити деякі відмінності між новим значенням фізичного шуму та витягнутим значенням фізичного шуму шляхом використання ступеня кореляції та вимоги граничного ступеня кореляції. US2005/0257064 описує підходящий статистичний спосіб для розрахунків ступеня кореляції або подоби між двома цифровими сигнатурами, отриманими з вимірювань фізичних ознак волокнистого середовища.

40 Можливо, щоб етапи 329 і 331 виконував або користувач 601, або перевірочний центр 114. Якщо перевірочний центр надав користувачеві 601 УІП, кінцевий користувач може встановити справжність виробу на основі значення фізичного шуму. Аналогічно, якщо перевірочному центру 114 надано новий фізичний ключ, перевірочний центр може встановити справжність виробу на основі значення фізичного шуму.

45 Для відтворення значення системного шуму має бути відновлено таємний ключ. На етапі 333 за допомогою УІП і ІГК перевірочний центр 114 здатний витягти динамічний ключ 219 і активний статичний ключ 209 із записів, збережених у перевірочному центрі. Таємний ключ може потім бути відновлено за допомогою УІП 221, динамічного ключа 219 і активного статичного ключа 209. На етапі 335 нове значення системного шуму відтворюють шляхом хешування УІП і таємного ключа. На етапі 337 нове значення системного шуму порівнюють зі значенням системного шуму, витягнутим на етапі 325. Якщо нове значення системного шуму та витягнуте значення системного шуму ідентичні, виріб може бути визначений як справжній на етапі 339.

50 В одному варіанті здійснення для того, щоб виріб вважати справжнім, потрібні порівняння як значення фізичного шуму, так і значення системного шуму. Проте, за бажанням, можна дозволити встановлення справжності на основі тільки однієї із цих перевірок.

55 З отриманого активного статичного ключа 209 можна визначити виробничий центр 103, 105, 107, у якому було виготовлено виріб, оскільки активні статичні ключі переважно зберігають у перевірочному центрі разом з деталями їх зв'язаних виробничих центрів. З отриманого динамічного ключа 219 можна визначити інформацію про партію для виробу, оскільки динамічні ключі переважно зберігають у перевірочному центрі разом зі зв'язаною інформацією про партію.

Таким чином, перевірочний центр 114 може одержувати з коду 221, відправленого від користувача 601, різні блоки інформації 603 про окремий виріб, а також перевіряти справжність виробу. Потім уся інформація 603, або вибрані її частини, включаючи вказівку того, є чи ні виріб справжнім, може бути відправлена користувачеві 601. Це показано на фіг. 1. Інформацію 603 переважно відправляють користувачеві 601 тим же способом, яким було надіслано оригінальний код.

Фіг. 5 представляє процес маркування згідно з другим варіантом здійснення винаходу. У способі, представленому на фіг. 5, роблять два захищені ідентифікатори: один з яких засновано на значенні 225 системного шуму, а інший засновано на значенні 227 фізичного шуму. Значення 225 системного шуму з'єднують з УІП 221 на етапі 341. Комбінація значення системного шуму та значення фізичного шуму потім шифрують із ЗКГК 231 на етапі 343, щоб зробити перший ID 241, як у першому варіанті здійснення, представленому на фіг. 3. Перший ID 241 потім з'єднують з ІГК на етапі 345 і шифрують з глобальним ключем 235 на етапі 347, щоб зробити перший захищений ID 271. Значення 227 фізичного шуму з'єднують з УІП на етапі 221, щоб зробити другий ID 261. Другий ID шифрують з глобальним ключем 235 на етапі 353, щоб зробити другий захищений ID. Виріб потім може маркуватися на етапі 355 першим захищеним ID 271 і другим захищеним ID 281 або відміткою або відмітками, отриманими з комбінації першого захищеного ID 271 і другого захищеного ID 281.

Фіг. 6 представляє етапи, які виконуються для встановлення справжності виробу, маркованого за допомогою процесу, представленого на фіг. 5. На етапі 401 відмітка або відмітки зчитує користувач, і користувач одержує перший захищений ідентифікатор 271 і другий захищений ідентифікатор 281. На етапі 403, глобальний ключ 235 використовують для одержання значення 227 фізичного шуму, першої копії УІП 221, першого ID 241 і ІГК 233. Якщо користувач має глобальний ключ 235, користувач може встановити справжність виробу на основі другого захищеного ідентифікатора автономно, тобто не вимагаючи з'єднання з перевірочним центром. Користувач генерує новий фізичний ключ на етапі 407 і його хешують з УІП для генерування нового значення фізичного шуму на етапі 409. Користувач може порівнювати нове значення фізичного шуму зі значенням фізичного шуму, витягнутим на етапі 403, на етапі 411. Як описано з посиланням на фіг. 3, виріб може вважатися справжнім на етапі 419, якщо нове значення фізичного шуму дорівнює або значною мірою подібно витягнутому значенню фізичного шуму.

На етапі 405 ІГК використовується перевірочним центром для одержання ЗКГК 231, і ЗКГК використовується для дешифрування першого ID 241, щоб виявити системний шум і другу копію УІП. На етапі 408 друга копія УІП необов'язково порівнюється з другою копією УІП для перевірки. На етапі 423 перевірочний центр 114 одержує динамічний ключ 219 і активний статичний ключ 209 за допомогою ІГК і УІП. На етапі 415 нове значення системного шуму генерують шляхом спочатку відновлення таємного ключа з УІП, динамічного ключа та статичного ключа, і потім шляхом хешування таємного ключа з УІП. На етапі 417 нове значення системного шуму порівнюють зі значенням системного шуму, витягнутим на етапі 405. Якщо вони ідентичні, справжність виробу можна встановити на етапі 419. Як і у випадку варіанта здійснення, представленого на фіг. 3, для того щоб виріб вважався справжнім, може вимагатися встановлення справжності, основане як на значенні системного шуму, так і на значенні фізичного шуму.

Хоча винахід було описано з посиланням на виготовлення сигарет, слід розуміти, що винахід можна застосовувати для будь-яких продуктів, які вимагають встановлення справжності, таких як лікарські препарати, алкогольні напої та предмети розкоші.

ФОРМУЛА ВИНАХОДУ

1. Спосіб маркування промислового виробу, який включає: створення унікального ідентифікатора продукту (УІП) для промислового виробу;
створення одного або декількох ключів (209, 219) шифрування;
генерування таємного ключа (223) за допомогою унікального ідентифікатора продукту та одного або декількох ключів шифрування;
генерування значення (225) системного шуму за допомогою таємного ключа та унікального ідентифікатора продукту;
генерування фізичного ключа (207) з виміряної фізичної ознаки промислового виробу;
генерування значення (227) фізичного шуму за допомогою фізичного ключа та унікального ідентифікатора продукту,

при цьому для утворення значення системного шуму та значення фізичного шуму використовують перетворення, заміщення, табличне заміщення та індексування або криптографічну хеш-функцію на комбінації унікального ідентифікатора продукту з таємним ключем і на комбінації унікального ідентифікатора продукту з фізичним ключем;

5 генерування захищеного ідентифікатора, що отримано з таємного ключа та фізичного ключа або що містить їх; при цьому захищений ідентифікатор одержують зі значення системного шуму або ж він включає значення системного шуму, і при цьому захищений ідентифікатор одержують зі значення фізичного шуму або ж він включає значення фізичного шуму, і розміщення відмітки на промисловому виробі, при цьому відмітка містить захищений ідентифікатор або ідентифікатор, отриманий із захищеного ідентифікатора.

10 2. Спосіб за п. 1, який **відрізняється** тим, що захищений ідентифікатор містить унікальний ідентифікатор продукту.

3. Спосіб за п. 2, який **відрізняється** тим, що етап генерування захищеного ідентифікатора включає генерування першого ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням системного шуму та генерування захищеного ідентифікатора шляхом шифрування першого ідентифікатора разом зі значенням фізичного шуму.

4. Спосіб за п. 3, який **відрізняється** тим, що:

етап генерування першого ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням системного шуму здійснюють шляхом шифрування

20 заплутувальним ключем генератора коду; перший ідентифікатор потім з'єднують зі значенням фізичного шуму та ідентифікатором генератора коду;

комбінацію першого ідентифікатора, значення фізичного шуму та ідентифікатора генератора коду потім шифрують із застосуванням глобального ключа для одержання захищеного ідентифікатора.

25 5. Спосіб за п. 4, який **відрізняється** тим, що заплутувальний ключ генератора коду є конкретним для генератора коду, в який його було попередньо завантажено, і при цьому глобальний ключ є загальним для всіх виробничих центрів.

6. Спосіб за п. 3, який додатково включає встановлення справжності промислового виробу в перевірному центрі, при цьому етап встановлення справжності включає:

ідентифікацію відмітки на виробі; дешифрування відмітки для одержання першого ідентифікатора та значення фізичного шуму; дешифрування першого ідентифікатора для одержання унікального ідентифікатора продукту та значення системного шуму;

35 генерування нового фізичного ключа з виміряної фізичної ознаки промислового виробу; генерування нової копії значення фізичного шуму шляхом виконання хеш-функції на новому фізичному ключі та отриманому унікальному ідентифікаторі продукту;

порівняння нової копії значення фізичного шуму з отриманим значенням фізичного шуму; і надання вказівки, чи отримане значення фізичного шуму є ідентичним новій копії значення

40 фізичного шуму або чи корелює воно з нею.

7. Спосіб за п. 6, який **відрізняється** тим, що етап встановлення справжності додатково включає:

генерування нової копії таємного ключа з унікального ідентифікатора продукту та одного або декількох ключів шифрування;

45 генерування нової копії значення системного шуму шляхом виконання хеш-функції на новій копії таємного ключа та унікальному ідентифікаторі продукту; порівняння нової копії значення системного шуму з отриманим значенням системного шуму; і надання вказівки, чи ідентичні нова копія значення системного шуму та отримане значення системного шуму.

50 8. Спосіб за п. 2, який **відрізняється** тим, що етап генерування захищеного ідентифікатора включає генерування першого захищеного ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням системного шуму;

генерування другого захищеного ідентифікатора шляхом шифрування унікального ідентифікатора продукту разом зі значенням фізичного шуму; і

55 розміщення відмітки на промисловому виробі, при цьому відмітка містить перший і другий захищені ідентифікатори або ідентифікатор чи ідентифікатори, отримані з першого та другого захищених ідентифікаторів.

9. Спосіб за п. 8, який **відрізняється** тим, що:

значення системного шуму з'єднують з унікальним ідентифікатором продукту;

- комбінацію значення системного шуму та унікального ідентифікатора продукту потім шифрують із застосуванням заплутувального ключа генератора коду, для одержання першого ідентифікатора;
- перший ідентифікатор потім з'єднують з ідентифікатором генератора коду і шифрують із застосуванням глобального ключа, для одержання першого захищеного ідентифікатора;
- значення фізичного шуму з'єднують з унікальним ідентифікатором продукту, для одержання другого ідентифікатора;
- другий ідентифікатор шифрують із застосуванням глобального ключа, для одержання другого захищеного ідентифікатора.
10. Спосіб за п. 8, який додатково включає встановлення справжності промислового виробу в перевірному центрі, при цьому етап встановлення справжності включає:
- ідентифікацію відмітки на виробі;
- дешифрування відмітки для одержання унікального ідентифікатора продукту, системного шуму та фізичного шуму;
- 15 генерування нової копії таємного ключа з унікального ідентифікатора продукту та одного або декількох ключів шифрування;
- генерування нової копії значення системного шуму шляхом виконання хеш-функції на новій копії таємного ключа та унікальному ідентифікаторі продукту;
- порівняння нової копії значення системного шуму з отриманим значенням системного шуму;
- 20 генерування нового фізичного ключа з вимірної фізичної ознаки промислового виробу;
- генерування нової копії значення фізичного шуму шляхом виконання хеш-функції на новому фізичному ключі та отриманому унікальному ідентифікаторі продукту;
- порівняння нової копії значення фізичного шуму з отриманим значенням фізичного шуму; і
- надання вказівки, чи ідентична нова копія значення системного шуму отриманому значенню системного шуму та чи ідентична нова копія значення фізичного шуму отриманому значенню фізичного шуму або чи корелює з нею.
- 25 11. Спосіб за будь-яким попереднім пунктом, який **відрізняється** тим, що один або кілька ключів шифрування містять статичний ключ і динамічний ключ, і при цьому новий динамічний ключ створюють для кожної партії промислових виробів.
- 30 12. Спосіб за будь-яким попереднім пунктом, який **відрізняється** тим, що унікальний ідентифікатор продукту містить інформацію, що ідентифікує партію виробів, до якої належить виріб.
13. Спосіб за будь-яким попереднім пунктом, який **відрізняється** тим, що значення шуму являє собою значення хешу або значення хешу з ключем, або значення чи послідовність символів, отримані безпосередньо зі значення хешу та таємного ключа.
- 35 14. Спосіб за будь-яким попереднім пунктом, який **відрізняється** тим, що виміряна фізична ознака промислового виробу заснована на текстурі поверхні цього промислового виробу.
15. Пристрій для маркування промислового виробу, який містить:
- генератор ключа, виконаний з можливістю генерувати ключі шифрування;
- 40 генератор коду, виконаний з можливістю генерувати унікальний ідентифікатор продукту для кожного промислового виробу;
- генератор фізичного ключа, виконаний з можливістю генерувати фізичні ключі з вимірної фізичної ознаки кожного промислового виробу;
- засіб обробки, виконаний з можливістю:
- 45 генерувати таємний ключ для кожного промислового виробу за допомогою унікального ідентифікатора продукту й одного або декількох ключів шифрування;
- генерувати значення системного шуму для кожного промислового виробу шляхом виконання певної хеш-функції на таємному ключі та унікальному ідентифікаторі продукту;
- генерувати значення фізичного шуму для кожного промислового виробу шляхом виконання певної хеш-функції на фізичному ключі та унікальному ідентифікаторі продукту;
- 50 генерувати захищений ідентифікатор, що отримано з таємного ключа та фізичного ключа або що містить їх; при цьому захищений ідентифікатор одержують зі значення системного шуму або ж він включає значення системного шуму, і при цьому захищений ідентифікатор одержують зі значення фізичного шуму або ж він включає значення фізичного шуму, і
- 55 маркер для маркування кожного промислового виробу захищеним ідентифікатором або ідентифікатором, отриманим із захищеного ідентифікатора.
16. Пристрій за п. 15, який **відрізняється** тим, що виміряна фізична ознака промислового виробу заснована на текстурі поверхні цього промислового виробу.

Fig. 1

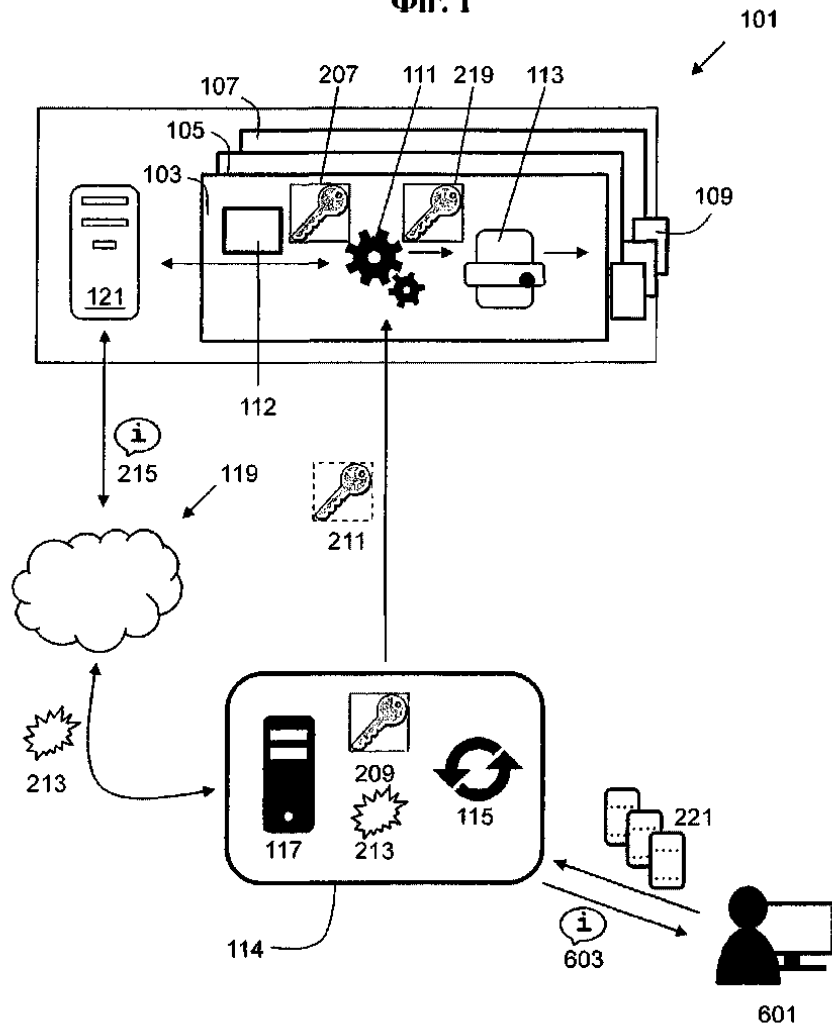
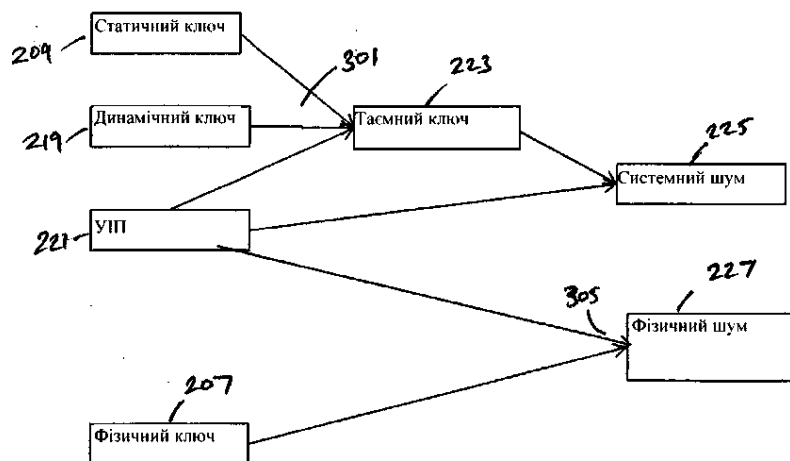
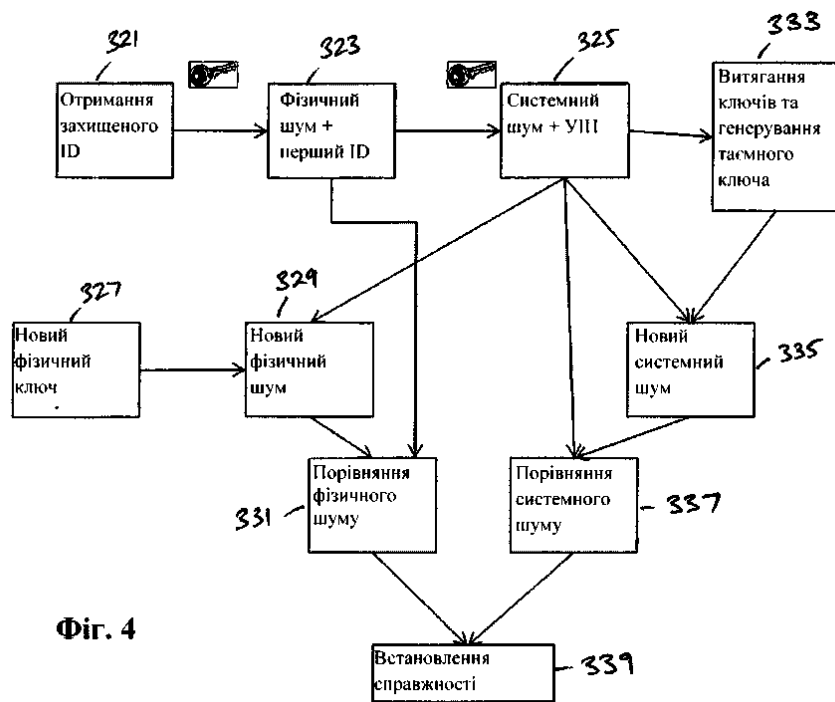
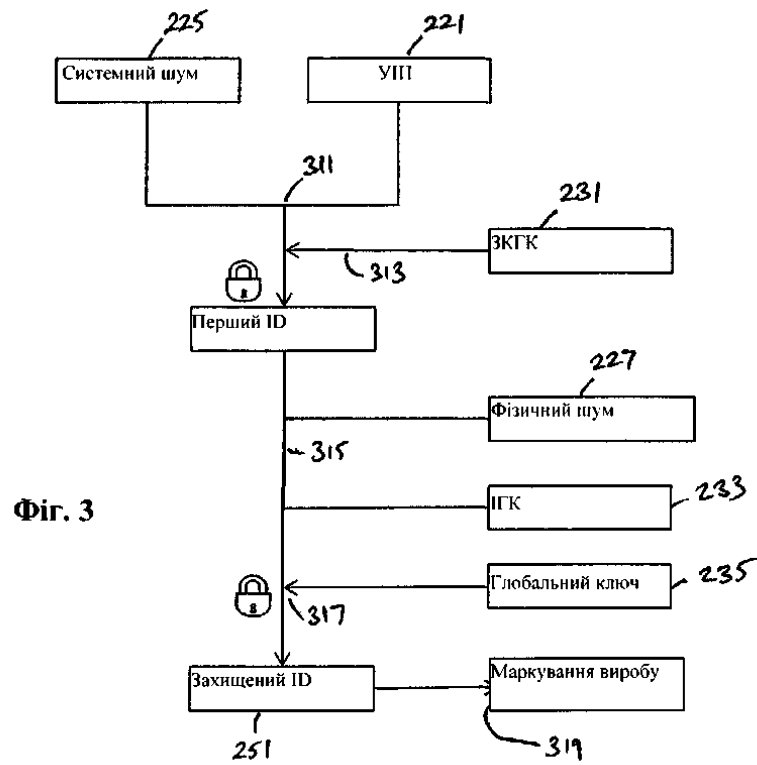
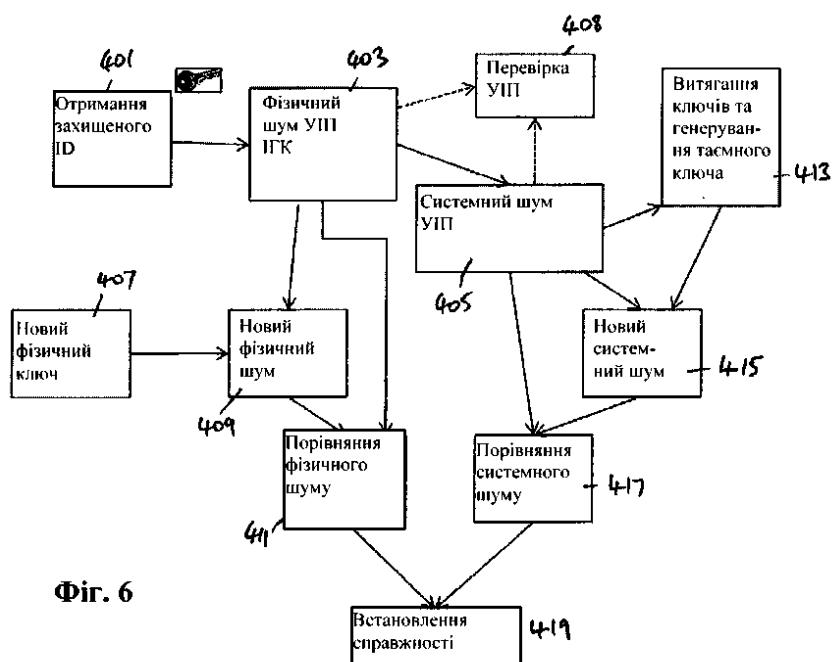
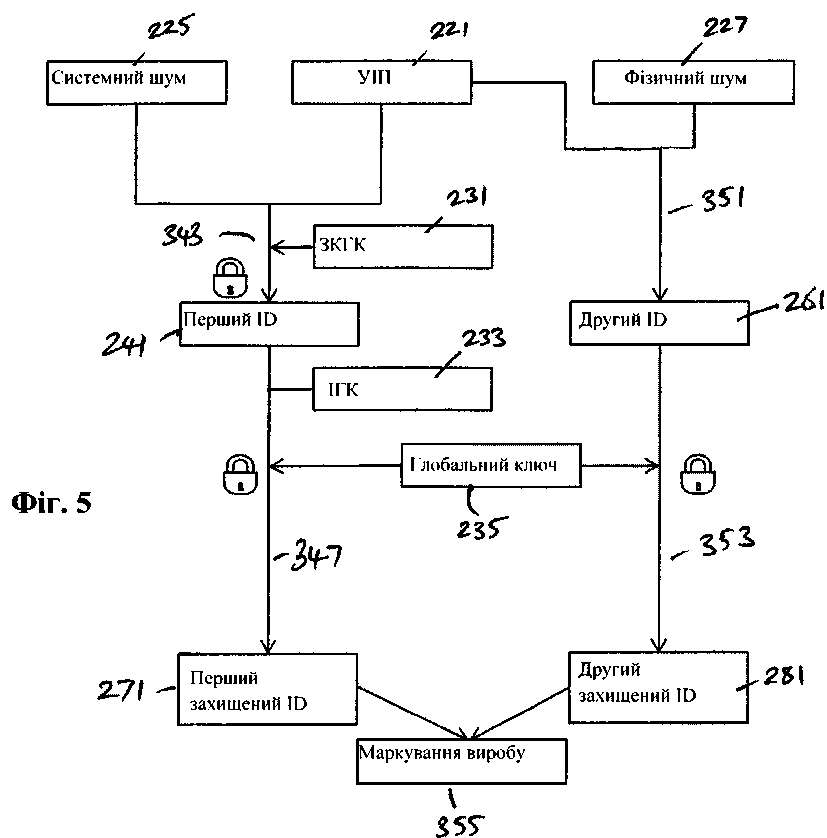


Fig. 2







Комп'ютерна верстка О. Рябо

Міністерство розвитку економіки, торгівлі та сільського господарства України,
вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601